NASA Procedural Requirements

NPR 8705.5
Effective Date: July 12, 2004
Expiration Date: July 12, 2009

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Subject: Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects

Responsible Office: Office of Safety and Mission Assurance

CHAPTER 4: Application of PRA

4.1 General Requirements

4.1.1 A PRA shall be comprehensive, balanced, and tailored (Requirement 33108).

4.1.1.1 A comprehensive PRA shall consider the complete environment and all factors that pertain to the system being assessed, including, as appropriate to satisfy its stated objective(s), the safety of the public, astronauts, pilots, and the NASA workforce; protection of high-value equipment and property; adverse impacts on the environment; national interests; and security (Requirement 33109).

4.1.1.2 A balanced PRA shall ensure that the scope considers issues of safety, operation, and mission assurance; is conducted at a level commensurate with the level of risk; and is timely to assist program/project management in limiting risk (Requirement 33110).

4.1.1.3 A tailored PRA shall ensure that the level of detail is commensurate with the complexity of the hazards, scope, and objective(s) of the mission/project being evaluated (Requirement 33111).

4.1.2 PRA implementation procedures shall reflect and incorporate the results of project risk analysis (Requirement 33112), including:

a. Identification of the elements of risk (initiators, hazards, scenarios, probabilities, and consequences) (Requirement 33113).

b. Recommended controls (preventive and mitigating features, compensatory measures) needed to reduce and manage risks (Requirement 33114).

4.2 PRA Throughout the Life Cycle Phases

A common misconception is that a PRA is not possible or useful when few data are available. In fact, this is precisely the situation when a PRA is most useful. The comprehensive and systematic nature of the assessment associated with a PRA is directly applicable to systems with the largest uncertainties. No PRA would be needed if all information required to ensure mission safety is known with certainty. Although a PRA is useful in all program/project life cycle phases, the type of information that is required and the types of scenarios modeled vary. This is illustrated in the following discussion of a typical program/project life cycle consisting of four phases: design, operation, upgrade, and decommissioning. This discussion demonstrates that, in all these phases, the assessment of comparative or relative risk, rather than its absolute value, will be most useful.

4.2.1 PRA in Design

Design generally seeks to optimize programs, missions, and/or systems to meet required objectives and functionality within technical, schedule, regulatory, and cost constraints. A good design effort generally develops technologically feasible configurations that meet required objectives and seeks options that best satisfy schedule and regulatory constraints while minimizing costs. PRAs are used to identify and quantify the risks associated with each option for input to management trade-off processes that include minimizing risk. Even if mission specific data

do not exist, failure rates and failure probabilities can be bracketed by comparisons with components where data do exist. When specific data do not exist, expert judgment data based on sound expert elicitation processes can be used to estimate top-level relative risk conclusions. Risk importance measures determined by a PRA will also serve to focus the evolution of the design.

4.2.2 PRA in Operation

During operation, especially for new programs and missions, there are many questions related to the anticipated success of the program or mission. A PRA performed prior to operation can serve to predict impacts to the program that could be detrimental to success. Thus, given that the design is acceptable from a safety perspective, a PRA for operations can focus on those aspects of risk that relate to system operability and maintenance and the performance of the mission. Risk importance measures determined by the PRA can be used to optimize procedures and resource allocations during operation. A PRA for operations can also include performance considerations and regulatory requirements. If there are problems meeting performance or regulatory requirements, PRA can identify modifications to hardware, software, and operational parameters that may be the appropriate solutions.

4.2.3 PRA in Upgrade

After operating a system for a while, experience is gained and improvements may be required. In addition, changing technology, obsolescence of components, and aging will play significant roles in the need for improvement or upgrades to a system. To this end, a PRA can identify upgrade options that minimize risk. Generally each upgrade will have its advocates. PRA provides an assessment tool for evaluating the relative risk benefits of alternative upgrade options.

4.2.4 PRA at End of Life or in Decommissioning

When a product is at the end of its useful life, it is important that its end of operation and subsequent dismantling and disposal be conducted cost-effectively, with due consideration to regulatory requirements and regard to the safety of the surrounding population and environment. A PRA can be effectively used to assess dismantling, decommissioning, and disposal options that minimize risks. Transitioning to a replacement system can also be included in this category if the replacement system is drastically different from the system being replaced, or if the transition is terminal. If the replacement system is an improvement, transitioning can be included as an upgrade as described in paragraph 3.4.3.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | AppendixA | ALL |

| NODIS Library | Program Management(8000s) | Search |

DISTRIBUTION:
NODIS